

UNITED STATES DISTRICT COURT

for the
Western District of OklahomaRMB
7/31/23

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)BLUE APPLE IPHONE SE (A2595), IMEI
354398682320726, located at HSI 3625 NW 56th St.,
Third Floor, Oklahoma City OK 73112

Case No. M-23- 588 -AMG

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A

located in the Western District of Oklahoma, there is now concealed (identify the person or describe the property to be seized):
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
21 U.S.C. § 841(a)(1)

Offense Description
Possession with intent to distribute a quantity of fentanyl

The application is based on these facts:
See attached Affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Ryan Belcher, Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date:

7/31/23


Judge's signature

City and state: Oklahoma City, Oklahoma

Amanda Maxfield Green, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA**

In the Matter of the Search of: (1) blue Apple iPhone SE (A2595), IMEI 354398682320726; and (2) a black BLU cell phone, IMEI 351464771851360; Currently Stored at the Homeland Security Investigations Oklahoma City Office

Case No. _____

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Ryan Belcher, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property—a list of electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant. I am a Special Agent with the Homeland Security Investigations (HSI) assigned to the Oklahoma City office; I have been employed by HSI since April 2015. As part of my duties as an HSI Special Agent, I am responsible for conducting investigations into violations of federal laws, including the

manufacturing and possession of controlled substances with the intent to distribute. I have received approximately 24 weeks of specialized training at the Federal Law Enforcement Training Center in the enforcement of federal laws. I have arrested, interviewed, and debriefed numerous individuals who have been involved and have personal knowledge of transporting and concealing narcotics, as well as, the amassing, spending, converting, transporting, distributing, money laundering and concealing of proceeds from narcotics trafficking and smuggling. I have participated in numerous investigations involving physical and electronic surveillance. I have testified in judicial proceedings concerning the prosecution for violations of laws related to the smuggling and trafficking of contraband, including controlled substances. I have been the affiant and participated on numerous federal search warrants.

3. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, and conversations with others who have personal knowledge of the events and circumstances described herein. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth every fact I, or others, have learned during the course of this investigation.

4. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 21 U.S.C. § 841(a)(1) (Drug

Conspiracy) and 18 U.S.C. § 924(c)(1)(A) (Possession of Firearms in Furtherance of a Drug Trafficking Crime) exists and is recorded on the devices described in Attachment A and will be located in the electronically stored information described in Attachment B.

Identification of the Devices to be Examined

5. The property to be searched is a (1) blue Apple iPhone SE (A2595), IMEI 354398682320726; and (2) a black BLU cell phone, serial number 5040018023016682;, (the “Devices”). The Devices are currently located at the HSI Oklahoma City office.

6. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

Probable Cause

7. On June 27, 2023, at approximately 6:50 p.m., while conducting patrol on U.S. Interstate 40, in Beckham County, Oklahoma, Oklahoma Bureau of Narcotics (OBN) Task Force Officer (TFO) B. Oden conducted a traffic stop on a maroon 2021, Nissan SUV, bearing Illinois License Plate 384797.

8. During the traffic stop, the driver was identified as Mina GRANADO, who was travelling with a male passenger in the vehicle, later identified as Anthony THOMAS. While speaking with GRANADO, TFO B. Oden noticed a strong odor of marijuana emitting from the vehicle. TFO B. Oden asked GRANADO to step back to his unit so he could issue her a warning for the traffic violations. There, TFO B. Oden

explained to GRANADO that he smelled marijuana coming from the vehicle and asked her if any marijuana was inside the vehicle. GRANADO stated the couple had smoked marijuana earlier that day. TFO B. Oden explained to GRANADO that he would be conducting a probable cause search of the vehicle due to the odor of marijuana.

9. At this time, an additional OBN Agent arrived to assist with the traffic stop. The male passenger in the vehicle, Anthony THOMAS, was advised a probable cause search of the vehicle would be conducted. THOMAS advised he was blind, so THOMAS was assisted from the vehicle. Upon assisting THOMAS from the vehicle, TFO B. Oden observed something concealed in THOMAS' sock. TFO B. Oden asked THOMAS about the bulge in his sock. THOMAS replied that it was medicine. The item was removed from THOMAS' sock and was found to be a five-dollar bill rolled up. Concealed within the bill were three blue pills stamped with "M30." "M30" pills are commonly found to be counterfeit oxycodone that contain fentanyl. Together, TFO B. Oden and the OBN Agent, conducted a probable cause search of the vehicle.

10. During the search of the vehicle, TFO B. Oden discovered a speaker that was still in the original packaging. The speaker box was noticeably heavier than it should be. The officers also discovered tools near the driver's seat that could be used to disassemble the speaker. Further inspection of the speaker revealed numerous items concealed within the speaker. The items discovered within the speaker were: three firearms, two clear bags containing blue pills, two bundles wrapped in silver packaging and two bags of

marijuana. The blue pills found in the speaker were similar to the ones found in THOMAS' sock and were also stamped "M30." After finding the drugs in the car, law enforcement seized the Devices and stored them as evidence.

11. Both GRANADO and THOMAS were arrested by OBN for multiple violations of Oklahoma law. GRANADO and THOMAS were booked into Beckham County Jail. It was discovered later that the two bundles wrapped in silver packaging contained more of the "M30" pills. Due to safety concerns regarding the pills containing fentanyl, a field test was not conducted on the pills. However, the "M30" pills discovered in the speaker box are consistent with pills commonly found to contain fentanyl. The mixture or substance containing fentanyl was later weighed and yielded an approximate weight of 921 grams.

12. On June 28, 2023, HSI Special Agent (SA) R. Belcher was notified of the incident. On that same date, SA Belcher, and Drug Enforcement Administration (DEA) TFO M. Dlugokinski interviewed GRANADO at the Beckham County Jail. Prior to the interview, GRANADO was advised of her rights, which she acknowledged, and waived her right to have an attorney present during the interview. During the interview, GRANADO admitted to travelling to Tempe, Arizona with THOMAS, where they purchased the pills, firearms, and marijuana from a man with the moniker "TG." GRANADO admitted to purchasing the speaker, with the intent to conceal the drugs and firearms, to transport them back to Illinois. GRANADO said that "TG" had given her the pills and if she made money from them, she would pay him via Cash App. GRANADO

told the investigators that she had bought weed from "TG" previously and utilized Cash App to pay him. GRANADO said that she had seen "TG" post M30 pills on his Snapchat account and that his Snapchat username was "TG."

13. SA Belcher asked GRANADO how many phones she had in the vehicle, and she stated she had two phones. GRANADO stated she had just purchased the iPhone and previously had an Android cell phone. SA Belcher asked if GRANADO had "TG"'s phone number and if it was under the contact name of "TG," and GRANADO confirmed that she had his number in her phone under "TG."

14. I know, based on my training and experience, that drug trafficking organizations routinely utilize cell phones in furtherance of their drug trafficking and money laundering activities. This use of cell phones almost always leaves behind evidence on the phone itself. This evidence includes communications with coconspirators, call records, location information for the user of the phone during the time crimes were committed, and videos/photographs of drugs, drug proceeds, receipts, or other logs. Further, I know that drug traffickers often utilize multiple cell phones and change cell phones to compartmentalize their illicit activities and thwart law enforcement.

15. Based on my training and experience, I know that Drug Trafficking Organizations (DTO) commonly depend upon cell phones and other electronic devices to communicate with one another. Furthermore, prior investigative experience has proven that conspirators associated with a DTO regularly utilize cell phones to advance their illicit

activities. Cell phones used by DTO members commonly provide key evidence in law enforcement's investigations, including call records, text messages, WhatsApp messages, photographs, videos, and location data.

16. The Devices are currently in storage at the HSI Oklahoma City office in Oklahoma City, Oklahoma. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of law enforcement.

Technical Terms

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in

electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. **Digital camera:** A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage

media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. **PDA:** A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. **Tablet:** A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the

Web, sending and receiving e-mail, and participating in Internet social networks.

- g. **IP Address:** An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- h. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

18. Based on my training, experience, and research, I know that each of the Devices have capabilities to allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and a PDA. I also know that each of the Devices is capable of connecting to and surfing the internet. In my training and experience,

examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

19. As set forth in **Attachment B**, the warrant I am applying for requests authorization for search and seizure of only those electronic devices which appear to be found in a location or under circumstances indicating they are not used exclusively for family use or use by children who may reside at the Subject Premises and therefore is limited to computers or electronic devices which are likely to contain the evidence sought by this application.

Electronic Storage and Forensic Analysis

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

21. I know that cellular telephones are often equipped with digital cameras and those phones possess the capability to transmit and/or store electronic images. I know that in many cases, cellular telephones maintain photographs of illegal activities. These photos are sometimes stored in their cellular phones and often are transmitted or sent from one electronic media device to another. I also know that cellular phones may also contain notes regarding potential illegal acts that are recorded by the subject who possesses the electronics. Furthermore, I know that text messages and emails are often used by two or

more persons to communicate information regarding illegal activities, between principals and co-conspirators of those crimes.

22. I know that cellular telephones are utilized by the majority of individuals in the United States and have become a staple of communication between individuals using text messaging, visual and audible communications (telephone calls and FaceTime type communications) as well as applications like “Whatsapp” and “GroupMe.” Additionally, individuals utilize their cellular devices to take pictures, keep notes, as a GPS (global positioning System) device, and even to conduct illicit or illegal activity. Communications on phones are kept for long periods and transferred from one phone to another when replaced. This is done through the use of Cloud storage and direct transfer conducted at the time of purchase or by the individual themselves. Individuals utilize this method as not to lose data that is stored on the phone such as contacts, photos, notes, and other important information to the individual. This data includes contacts used to conduct illegal activities to include drug trafficking and money laundering.

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to communicate about drug trafficking or associated money laundering, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

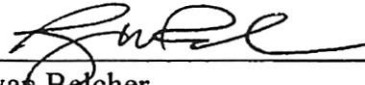
26. *Methods of examination.* In conducting this examination, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the Devices. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with stored cellular device data, such as pictures and videos, do not store as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications associated with a cellular device, as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications.

Consequently, often many communications in cellular device data that are relevant to an investigation do not contain any searched keywords.

Conclusion

27. Based on the information above, I submit that there is probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Ryan Belcher
Special Agent
Homeland Security Investigations

Subscribed and sworn on this 31st day of July 2023.

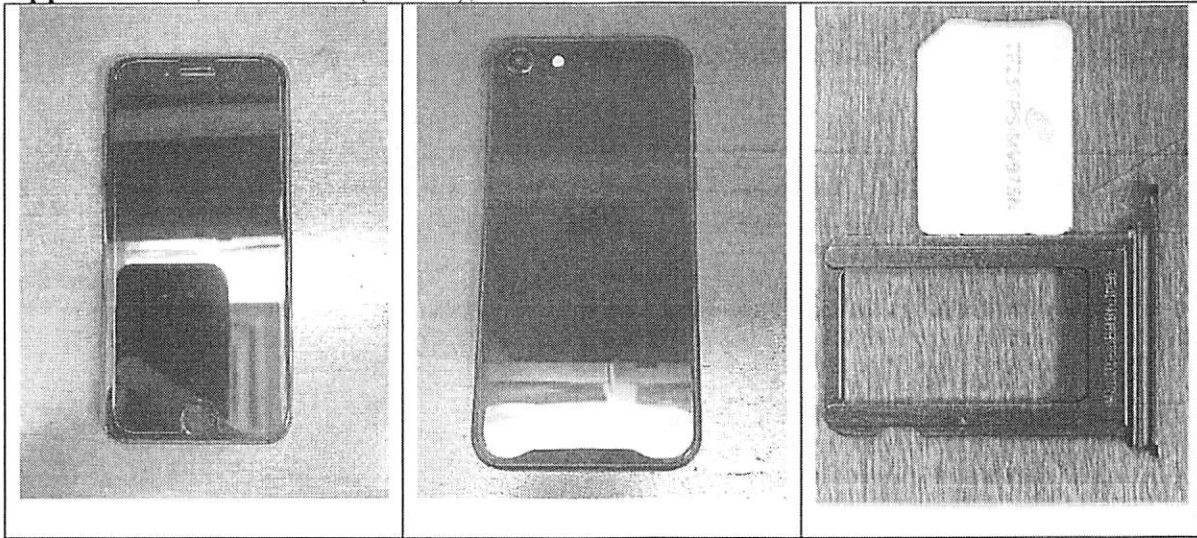


AMANDA MAXFIELD GREEN
U.S. Magistrate Judge

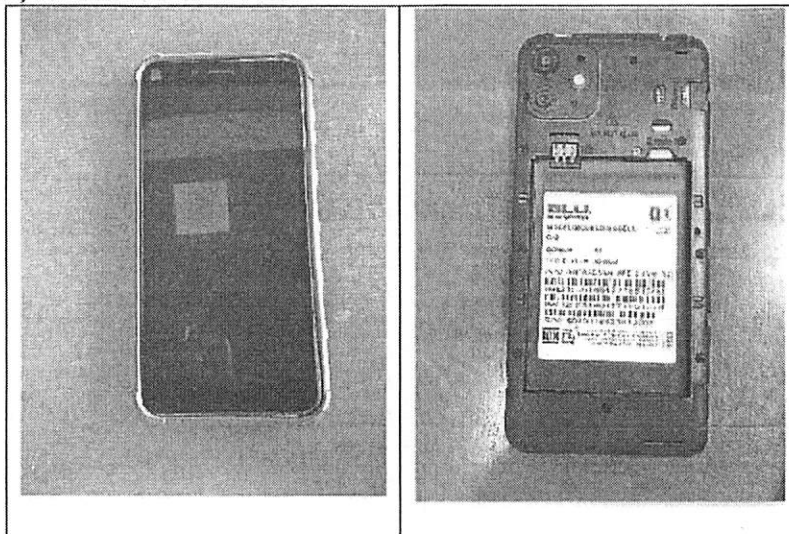
ATTACHMENT A

The property to be searched is a blue Apple iPhone, model SE (A2595), IMEI 354398682320726, and a black BLU cell phone, IMEI 351464771851360. The Devices are currently located in secure evidence storage at the HSI Oklahoma City office.

Apple iPhone, model SE (A2595), IMEI 354398682320726



BLU cell phone, IMEI 351464771851360



ATTACHMENT B

Particular Things to be Seized

1. All evidence relating to violations of 21 U.S.C. § 841(a)(1) and 18 U.S.C. § 924(c)(1)(A), including but not limited to:
 - a. Any and all images, videos, and any other digital media content of Mina Granado or Anthony Thomas and/or their co-conspirators, relating to assets, or illegal drugs;
 - b. call logs, address books, GPS data, internet access, IP accounts, text messages, and email accounts;
 - c. lists of customers and related identifying information;
 - d. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
 - e. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
 - f. any information recording Mina Granado or Anthony Thomas' schedule or travels from June 2023, which correlates to the timeframe of their arrest on June 27, 2023;
 - g. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records documenting the use of the Internet Protocol addresses to communicated with e-mail servers, internet sites, and social media, including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

4. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied, or disclosed pursuant to this warrant in order to locate any evidence, fruits, and instrumentalities of violations of the above-listed federal criminal statutes. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents,

attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.